

# METHOD AND APPARATUS FOR USING CLIENT PUZZLES TO PROTECT AGAINST DENIAL-OF-SERVICE ATTACKS

## ABSTRACT

One embodiment of the present invention provides a system that protects a server against denial-of-service attacks. During operation, the server receives a request for service from a client. Note that the client can be distinguished from other clients, for example, by its source IP address. In response to this request, the server sends a random number,  $y$ , and an identifier,  $id_1$ , to the client, and allows the client to compute a preimage,  $x$ , such that  $y = h(x)$ . Upon receiving an answer from the client including the preimage  $x$  and an identifier,  $id_2$ , the server verifies that the identifier,  $id_1$ , sent to the client matches the identifier,  $id_2$ , received from the client. If the identifiers match, the server computes  $h(x)$ , and compares  $h(x)$  against  $y$ . If  $h(x) = y$ , the server performs the requested service for the client. In this way, the server avoids computing  $h(x)$  until the server receives the answer with a matching identifier.